



INTERNATIONAL PRELIMINARY EXAMINATION REPORT  
(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 90 450 a/ubr/ds	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP 02/07076	International filing date (day/month/year) 26.06.2002	Priority date (day/month/year) 26.06.2002
International Patent Classification (IPC) or both national classification and IPC H04L9/32		
Applicant TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
- ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
- These annexes consist of a total of sheets.

## 3. This report contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand  22.01.2004	Date of completion of this report  13.07.2004
Name and mailing address of the international preliminary examining authority:   European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer  Apostolescu, R  Telephone No. +49 89 2399-7950 

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. **PCT/EP 02/07076**

**I. Basis of the report**

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

**Description, Pages**

1-19 as originally filed

**Claims, Numbers**

1-10 as originally filed

**Drawings, Sheets**

1/5-5/5 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. **PCT/EP 02/07076**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

*(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Yes: Claims	1-10
	No: Claims	
Inventive step (IS)	Yes: Claims	1-10
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-10
	No: Claims	

2. Citations and explanations

**see separate sheet**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 02/07076

**Re Item V**

**Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

Reference is made to the following documents:

- D1: 'TDMA Third Generation Wireless Authentication, Encryption of Signaling Information/User Data, and Privacy' TIA/EIA STANDARD, [Online] 31 March 2000 (2000-03-31), pages 1-62, XP002231163 USA Retrieved from the Internet: <URL: [http://ftp.tiaonline.org/uwc136/136-5 10-B.pdf](http://ftp.tiaonline.org/uwc136/136-5%20-B.pdf)> [retrieved on 2003-02-14]
- D2: US-A-5 241 598 (RAITH KRISTER A) 31 August 1993 (1993-08-31)
- D3: US-A-5 091 942 (DENT PAUL) 25 February 1992 (1992-02-25)

1. The present invention is directed to a method of controlling a network entity of a mobile communication network (claim 1), a mobile station arranged to exchange encrypted messages with a mobile communication network (claim 8) and a network entity of a mobile communication network (claim 10).

Document D1 is a standard of TIA directed to authentication and encryption of signaling information and user data in a TDMA wireless network.

Documents D2 and D3 describes the process of authentication of a mobile and a base station, and the parallel keystream generation in the mobile and the base station.

The problem is to disclose an improved method for operating a network entity of a mobile communication network and a mobile station that are able to exchange encrypted messages, and which both are arranged to conduct respective encryption key generation procedures in parallel.

Claim 1 of the present invention discloses a method of controlling a network entity and a mobile station which exchange encrypted messages, wherein if the network entity is unable to decrypt a received encrypted message it sends a triggering message to the mobile station, whereupon the mobile station interrupts the ongoing message exchange procedure in order to initiate an encryption key generation procedure.

The apparatuses disclosed in claims 8 and 10 correspond to the method disclosed in claim 1.

The advantage of the present invention lies in the fact that the mobile station does not wait until the ongoing message exchange procedure comes to an end by itself, e.g. by a time-out. With the sending of a predetermined triggering message from the network entity to the mobile station, a new encryption key generation is initiated. Thereby, an unnecessary loss of time for performing encryption key generation procedures in the network entity and mobile station is avoided.

The characterising features of the invention as disclosed in the claims are not anticipated by the prior art cited by the ISR.

Therefore, it is considered that independent claims 1 (method), 8 and 10 (apparatus) relate to new and inventive subject-matter (Articles 33 (2) and (3) PCT), since the prior art does not disclose or suggest the specifically claimed method of controlling a network entity of a mobile communication network and a mobile station according to claim 1 and does not disclose or suggest the specifically claimed features of the apparatus claims 8 and 10.

All other claims are dependent on one of these claims and therefore also meet the requirements for novelty and inventive step (Article 33(1) - (3) PCT).

**Remarks:**

1. The expression "the discussion of TIA/EIA-136 in the introduction is herewith incorporated into the disclosure of the invention" contravenes Rule 5.1 PCT (see also PCT Guidelines II-4.17).
2. A document reflecting the prior art described on pages 2 and 3, is not identified in the description (Rule 5.1(a)(ii) PCT).  
  
Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D2 and D3 is not mentioned in the description, nor are these documents identified therein.
3. Independent claims 1, 8 and 10 are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art (document D2 or D3) being placed in the preamble (Rule 6.3(b)(I) PCT) and with the remaining features being included in the characteris-

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

---

International application No. PCT/EP 02/07076

ing part (Rule 6.3(b)(ii) PCT).

4. On page 17, line 26 is a clerical mistake (Bomain-B).